



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/803,590
Filing Date: March 18, 2004
Appellant(s): OKUNSEINDE ET AL.

Okunseinde et al.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on April, 06, 2010 appealing from the Office action mailed on November 13, 2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

1. Claims canceled: 9-27 and 30
2. Claims withdrawing from consideration but not canceled: NONE
3. Claims pending: 1-8, 28-29, and 31-34
4. Claims allowed: NONE
5. Claims objected as allowable subject matter: 3 and 5
6. Claims rejected: 1-4, 6-8, 28, 29, and 31-34

(4) Status of Amendments After Final

Because the appellant's amendment to the claims filed on February 09, 2010 after the Final Office Action mailed on November 13, 2009 changes scopes of the claims, the examiner has not entered the amended claims after Final. As amended in claim 1, there is deference between claimed features of "at each of the source device and the at least one intermediate

device" as filed before final and "at the source device and at each of the at least one intermediate device" as filed after final.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner.

The rejection of claims 1, 3, and 5 under 35. U.S. C. §112, second paragraph as being indefinite has been withdrawn.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief are incorrect. It contains in claim 1 "at the source device and each of the at least one intermediate device" as amended after final on February 09, 2010 instead of "at each of the source device and at the at least one intermediate device" as filed before final on July 23, 2009.

(8) Evidence Relied Upon

20050188072

Lee

08-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-2, 4, 6-8, 28-29 and 31-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Suzuki (US. Pub. No.: US 2004/0259529) in view of Lee, IV et al. (Hereinafter referred to as Lee, US. Pub. No.: 2005/0188072).

As per claim 1:

Suzuki discloses a method, comprising:

determining security information associated with a object, wherein the security information is inserted in a header of the object and the object is to be transmitted from a source device to a target device along a transmission path that includes at least one intermediate device (0008; 0011-0012; Figure 2: Terminals A-D; Authentication header);

determining, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, whether a next

device in the transmission path to which the object is to be transmitted provides a security in the header of the object (0011; 0021; 0050; 0073-0074);

transmitting, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, the object to the next device in the transmission path in response to determining that the next device provides security in the header of the object (0044; 0050; 0073-0074).

Suzuki does not explicitly disclose security information is associated with a transaction object and providing a level of security indicated by at least a portion of the security information. Lee, in analogous art, however, disclose security information is associated with a transaction object (0028; 0054) and providing a level of security indicated by at least a portion of the security information (0043; security specific policy; 0054; 0094; level of policy application; 0106-0107). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Suzuki to include security information is associated with a transaction object and providing a level of security indicated by at least a portion of the security information. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do to dynamically construct a protocol to facilitate communication between nodes and across multiple nodes and utilize policies associated with the nodes to specify protocol properties of the nodes and select a policy expression in a policy related to a node by another node to construct a protocol between the two nodes as suggested by Lee in (0007).

As per claim 2:

Lee discloses the object is a business object, and wherein determining next device in the transmission path provides the level of security comprises: transmitting to the next device in the transmission path information representative of the level of security that is desired; and receiving a response from the next device in the transmission path indicating that the next device in the transmission path provides the desired level of security (0011; 0034; 0037).

As per claim 4:

Lee discloses the security information comprises determining security information relating to at least one of connection information, class information, trusted entities information, and logging capability information (0068-0069).

As per claim 6:

Lee discloses determining an alternative intermediate device along a different transmission path that is adapted to provide provides the level of security represented required by the at least a portion of the security information in response to determining that the adjacent intermediate next device in the transmission path does not adapted to provide the level of security required by the at least a portion of the security information (0083-088; 0100).

As per claim 7:

Lee discloses sending a message to the next device in the transmission path instructing the next device to execute at least one module that allows the next device to provide the level of security required by the at least a portion of the security information (0083-088).

As per claim 8:

Suzuki discloses determining the security information comprises determining the security information in response to receiving the object from at least one of a previous device or a source device in the transmission path (0011; 0021; 0050; 0073-0074).

As per claim 31:

Lee discloses at least one intermediate device includes at least a first intermediate device and a second intermediate device;

wherein determining if a next device in the transmission path provides a level of security required by the at least a portion of security information includes performing the determining at the source device, wherein the next device is the first intermediate device (0010; 0021; 0083-088);

wherein transmitting the object to the next device comprises transmitting the object to the first intermediate device, and wherein in response to determining that the next device provides the level of security and in response to determining that the first intermediate device provides the level of security (0083-088; 0094);

determining, at the first device, is second device of the plurality of intermediate devices that is adjacent the first device provides the level of security indicated by the at least a portion of the security information (0094; 0104; 0108; Figure 5: 500),

transmitting the object to the second device of the plurality of intermediate devices in response to determining that the second device provides the level of security; and transmitting the object to the target device from the second device (0094; 0104; 0108; Figure 5: 500).

As per claim 32:

Lee discloses determining an alternative intermediate device along a different transmission path that provides the level of security represented in response to determining that at least one of the first intermediate device and the second intermediate device in the transmission path does not provide the level of security (0054; 0100).

As per claim 33:

Lee discloses the at least one intermediate device includes a plurality of intermediate devices;

wherein determining if an adjacent intermediate a next device in the transmission path is adapted to provide provides a level of security comprises determining, at a previous device in the transmission path, a security level for each intermediate device of the plurality of intermediate devices (0084; 0094; 0100);

wherein transmitting the object to the adjacent intermediate next device in the transmission path in response to determining that the adjacent intermediate next device is

adapted to provide the level of security: comprises transmitting the object to each of the plurality of intermediate devices in the transmission path in response to determining that each of the plurality of intermediate devices is adapted to provide provides the level of security; further comprising: transmitting the object to the target device (0084; 0094; 0100).

As per claim 34:

Lee discloses the object is one of a plurality of objects of the transaction, and wherein at least two of the objects in the plurality of objects have different security information in their respective headers identifying different levels of security required to be provided by devices along corresponding transmission paths to receive the at least two objects (0083-088; 0100).

As per claim 28:

Suzuki discloses a method, comprising:

receiving, at a first device along a transmission path from a source device to a target device, a request from a second device along the transmission path desiring to transmit an object to a third device, wherein the request includes security information associated with the object, the security information being provided in a header of the object (0008; 0011-0012; Figure 2: Terminals A-D; Authentication header);

determining if the first device is adapted to provide a security identified by the security information in the header of the object; and transmitting an indication to the second device based on determining if the first device provides the security identified by the security information (0011; 0021; 0050; 0073-0074); and

receiving, in the first device, the object from the second device only in response to the first device transmitting an indication that the first device the security information (0044; 0050; 0073-0074).

Suzuki does not explicitly disclose providing a level of security indicated by at least a portion of the security information. Lee, in analogous art, however, disclose providing a level of security indicated by at least a portion of the security information (0043; security specific policy; 0054; 0094; level of policy application; 0106-0107). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Suzuki to include providing a level of security indicated by at least a portion of the security information. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do to dynamically construct a protocol to facilitate communication between nodes and across multiple nodes and utilize policies associated with the nodes to specify protocol properties of the nodes and select a policy expression in a policy related to a node by another node to construct a protocol between the two nodes as suggested by Lee in (0007).

As per claim 29:

Lee discloses configuring the first device with at least one module that provides the level of security (0083-088).

Allowable Subject Matter

3. Claims 3 and 5 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims and in addition if each and every rejection and objection of given above for this claim is overcome.

The following is a statement of reasons for the indication of allowable subject matter: Claim 3 includes the following features which are not taught or further suggested and would not have been obvious over prior arts of record as a whole either taken alone or in combination and with particular features of: prompting the next device in the transmission path to execute one module that allows the next device in the transmission path to prove the desired security level and comparing a list of trusted devices in a header portion of transmitted header objects that comprises an object handler module as defined and described in claim 3.

(10) Response to Argument

A. Rejection under 35 U.S.C. § 1121 Second Paragraph

The rejection of claims 1, 3, and 5 under 35. U.S. C. §112, second paragraph as being indefinite has been withdrawn

B. Rejection under 35 U.S.C. § 103(a)

Regarding Independent Claims 1 and 28

The appellant argues that *"Suzuki is not concerned with determining whether a next device along a transmission path provides a level of security indicated by at least a portion of the security information in the header of an object being transmitted"* in pages 7 and 10 of the appeal brief and the appellant also argues that *"regarding the specific features of claim 1 with regard to determining, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, whether a next device in the transmission path to which the object is to be transmitted provides a level of security indicated by at least a portion of the security information in the header of the object..... there is no teaching or technical rationale provided in these, or any other, sections of Lee regarding the specific features of transmitting, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, the object to the next device in the transmission path in response to determining that the next device provides the level of security required by the at least a portion of the security information"* in page 13 of the appeal brief.

The examiner disagrees with the appellant's argument and analysis. During examination, the examiner gave the broadest reasonable interpretation to the claims in light of the specification, and accordingly the "at least one intermediate device" is interpreted and considered broadly as "an intermediate device" between a source device and a target device to constitute only three devices to form a path (a source device, an intermediate device and a target device). Further more, a broadest reasonable interpretation has been given also to the recited claimed feature of "determining a level of security provided by a next device (in effect a target device)

indicated by at least a portion of security information in the header of the object". The security level is broad enough to be any security function or rule or policy or a security key or even the device's identification as long as it matches with security as indicated in the header of the object.

Suzuki discloses this feature, at least in paragraphs 0011, 0021 0050 and 0069 by having and matching a key and a terminal identifier of a receiving terminal in the authentication header of a frame at a transmitting terminal and also by mutually authenticating the transmitting terminal and the receiving terminal. The receiving terminal validates the received authentication header to validate the transmitter and the transmitting terminal validates the receiving terminal and this mutual authentication is carried out in tandem form to include the intermediate devices as shown in Figure 1 of Suzuki (Figure 1: Terminal A and Terminal B are mutually authenticating each other, Terminal B and Terminal C are mutually authenticating each other, and Terminal C and Terminal D are mutually authenticating each other as data are transmitted from a source Terminal A to receiving Terminal D though intermediate Terminal B and Terminal C, where the payload data having authentication header as it traverse the path through Terminal B and C).

In the Final Office Action mailed on November 13, 2009, the examiner stated that Suzuki does not explicitly disclose security information is associated with a transaction object and providing a level of security indicated by at least a portion of the security information. Lee, in analogous art, however, discloses security information is associated with a transaction object (0028; 0054) and providing a level of security indicated by at least a portion of the security information (0043; security specific policy; 0054; 0094; level of policy application; 0106-0107). In Figure 5: 500; Lee discloses a source node 502, intermediate nodes 506 and 508 and

destination node 504. Lee also discloses a method and system for retrieving an intermediate node policy and a destination node policy, the intermediate node policy characterizing communication properties supported by an intermediate node and the destination node policy characterizing communication properties supported by a destination node, the intermediate node being between a source node and the destination node in a communication path (0010; 0019; 0034). Therefore, for the reasons given above, the examiner disagrees with the appellant's argument and analysis and they are not persuasive to overcome the prior arts in record and place claims 1 and 28 in condition for allowance.

Regarding Dependent Claims 2-8, 29, and 31-34

Claim 2: The appellant argues that Lee does not disclose "determining next device in the transmission path provides the level of security comprises: transmitting to the next device in the transmission path information representative of the level of security that is desired; and receiving a response from the next device in the transmission path indicating that the next device in the transmission path provides the desired level of security". However, the examiner disagrees with the appellant's argument because Lee discloses policy messages and policy expression are transmitted and received between each node across the transmission path to comply with application level security at each node (0093-0095). Therefore, for the reasons given above, the appellant's arguments are not persuasive to overcome the prior art in record.

Claims 6 and 32: The appellant argues that Lee does not determine an alternative device along a different transmission path that provides the level of, security required by the at least a portion of the security information in response to determining that the next device in the

transmission path does not provide the level of security required by the at least a portion of the security information". The examiner disagrees with the appellant's argument and analysis because Lee discloses in paragraph 0083 that routing through firewalls at each node in the path that may have policies related to data protocols that are preferred or available and/or required by the node in paragraphs 0084 and 0085, Lee discloses selecting and retrieving security policy expression at each node for the message to reach a destination from source through intermediate node. Therefore, for the reasons given above, the appellant's arguments are not persuasive to overcome the prior arts in record.

Claims 7 and 29: The appellant argues that Lee does not disclose sending a message to the next device in the transmission path instructing the next device to execute at least one module that allows the next device to provide the level of security required by the at least a portion of the security information. The examiner disagrees with the appellant's argument and analysis because as shown above Lee discloses the alleged feature in paragraphs [0083-0088]. Therefore, for the reasons given above, the appellant's arguments are not persuasive to overcome the prior art in record.

Claim 31: The appellant argues that the examiner changed position by citing Lee for claims 31. The examiner disagrees with the appellant argument because the argument is just a general allegation instead of showing distinction between claimed features and cited prior art. The examiner states that Lee discloses the alleged feature of claim 31 in paragraphs [0021; 0083-0088; 0094 and 00104-0105]. Particularly Lee discloses in paragraph [0104]. The retrieving operation 604 then sends the created policy request to the first node in the list. The first node in the list removes a policy level (related to the first node) from the message and forwards the

request message on to the next node. The next node receives the policy request message and, if the request is for the node's policy, that node sends back its policy. Otherwise, the request is forwarded on to the next node. In paragraph [0105] Lee discloses the retrieving operation 604, the selecting operation 606, the determining operation 608, the inserting operation 610, the determining operation 612, and the creating operation 614 continue until the policy of each node in the multiple-node communication path is retrieved and compatible policy expressions are selected from each of the policies. Thus, a compatible policy expression is selected corresponding to each of the policies and each of the nodes. Therefore, for the reasons given above, the appellant's arguments are not persuasive to overcome the prior arts in record.

Claim 33: The appellant argues that Lee does not disclose "a security level for each intermediate device of the plurality of intermediate devices and transmission path in response to determining that each of the plurality of intermediate devices provides the level of security". The examiner disagrees with the appellant argument because the argument is just a general allegation instead of showing distinction between claimed features and cited prior art. The claimed features of claim 33 are disclosed in paragraphs [0084, 0094 and 0100] of Lee and therefore the appellant's arguments are not persuasive to overcome the prior arts in record.

Claim 34: The appellant argues that Lee does not disclose "at least two of the objects in the plurality of objects have different security information in their respective headers identifying different levels of security required to be provided by devices along corresponding transmission paths to receive the at least two objects". The examiner disagrees with the appellant argument because the argument is just a general allegation instead of showing distinction between claimed features and cited prior art. The claimed feature of claim 33 are disclosed in paragraphs [0083-

0084; 0094 and 0100] of Lee and obviously several objects or messages are transmitted from a source device to a destination device reach objects or messages requiring different security levels or information and therefore the appellant's arguments are not persuasive to overcome the prior art in record.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Techane J. Gergiso/

Primary Examiner, Art Unit 2437

Conferees:

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437